UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. JEREMY LEROY HELLER, JOSHUA S. PHY Defendants	Criminal No. 1:13-cr-383 Hon. Liam O'Grady Hearing Date: May 2, 2014

GOVERNMENT'S CONSOLIDATED OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS FOR IMPROPER VENUE

Defendants Heller (Dkt. No. 175) and Phy (Dkt. No. 177) each complain that the government has brought this case improperly in this District. Defendant Heller from Takoma Park, Maryland, and Defendant Phy from Gloucester, New Jersey, say they believe that venue would only be proper in any district from which a co-conspirator launched a DDoS attack, but not here in the Eastern District of Virginia. For that reason, they insist that the indictment be dismissed. Both defendants argue that no essential criminal acts were perpetrated here in this District in furtherance of the conspiracy they participated in. These Motions fail because, among other things:

- The computer crime statute here describes the essential criminal conduct as both the act of knowingly sending computer commands ***and*** intentionally causing damage to a protected computer. 18 U.S.C. § 1030(a)(5)(A);

- The damage caused by the co-conspirators included damage to computers here in the Eastern District of Virginia on several occasions during the conspiracy period.

In short, this conspiracy to violate Section 1030(a)(5)(A) is properly brought in the Eastern District of Virginia.

Factual Background

Between about September 16, 2010 through about January 2, 2011, the defendants participated in a worldwide conspiracy as part of the online group Anonymous in a campaign dubbed "Operation Payback" (or "Operation: Payback is a Bitch,") to engage in a coordinated series of cyber-attacks against victims. Operation Payback targeted victims worldwide, including governmental entities, trade associations, individuals, law firms, and financial institutions, which Anonymous claimed opposed its stated philosophy of making all information free for all, including information protected by copyright laws or national security considerations. As a result, the defendants launched, or attempted to launch, cyber-attacks (known as Distributed Denial of Service or "DDoS" attacks) against entities including the Recording Industry Association of America in the Eastern District of Virginia, the Motion Picture Association of America, the United States Copyright Office of the Library of Congress, Visa, MasterCard, and Bank of America (including computers at a data center in the Eastern District of Virginia), and caused millions of dollars in loss to these victims. They used a free and downloadable computer program called the Low Orbit Ion Cannon ("LOIC") (or similar tools), coordinated the time and target IP address to flood victim websites

with irrelevant internet traffic, and slowed access to the sites or effectively shut them down.

On October 3, 2013, a grand jury in the Eastern District of Virginia indicted the defendant with conspiring to intentionally cause damage to a protected computer, in violation of Title 18, United States Code, Section 371. Dkt. No. 1, at ¶ 3 (charging conspiracy to "knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage… without authorization, to a protected computer, with such damage… during the one-year period beginning on or about September 16, 2010 affecting ten or more protected computers and causing loss to victims resulting from the course of conduct affecting protected computers aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B).").

Legal Argument

Venue in a criminal case is proper in any district where the subject crime was committed. *United States v. Ebersole*, 411 F.3d 517, 524 (4th Cir.2005) (citations omitted). *See also* Fed R.Crim. P. 18. If Congress does not prescribe specific venue requirements for a particular crime, then venue is to "be determined from the nature of the crime alleged and the location of the act or acts constituting it." *United States v. Cabrales*, 524 U.S. 1, 6-7 (1998) (quoting *United States v. Anderson*, 328 U.S. 699, 703 (1946)). This determination must focus on the "essential conduct

elements" of the charged offense. *United States v. Bowens*, 224 F.3d 302, 311 (4th Cir. 2000).

A. The Essential Conduct Elements of Section 1030(a)(5)(A) Establishes Venue in the Eastern District of Virginia.

It appears undisputed that the statutes in question, namely Conspiracy (18 U.S.C. § 371), and Computer Fraud (18 U.S.C. § 1030(a)(5)(A)) do not contain specific venue provisions. Therefore, to determine proper venue, the essential conduct elements must be considered. *Bowens,* 224 F.3d at 311. The defendants describe the essential conduct elements for Section 1030(a)(5)(A) as "'knowingly caus[ing] the transmission of a program, information, code, or command' with the intent to cause damage." Heller MTD at 3; *see also* Phy MTD at 17. Despite Defendant Heller's admonition that this "analysis requires a close reading of statutory text," Heller MTD at 2, the defendants failed to read the statutory text closely enough.

1. Section 1030(a)(5)(A) Prohibits Not Only the Transmission of Programs, etc., But Also Damaging the Target Computer(s)

The relevant statute charged, 18 U.S.C. § 1030(a)(5)(A), provides that "whoever knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage[1] without authorization, to a protected computer," is guilty of an offense. This statute plainly

[1] "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Here, the entire purpose of a DDoS attack is to render a website inaccessible to users; sometimes DDoS attacks only accomplish making the website slow to respond – an impairment to the availability of information.

prohibits both the transmission to a protected computer ***and*** the causing of damage to the protected computer to which the transmission was directed. The word "and" in the statute joins both the transmission and the damage together as essential elements to form the offense.[2] With the correct reading of the statute, the essential conduct elements become: knowingly causes a transmission to a protected computer ***and*** intentionally causes damage without authorization to that protected computer. In short, the essential conduct elements of the offense include transmission and damage, not just the transmission as the defendants argue.[3]

2. Damage to Protected Computers From the Transmission of Computer Commands Occurred on Several Occasions in the Eastern District of Virginia During the Charged Conspiracy

The defendants are charged in the instant indictment with a single count of conspiracy (Section 371) to violate Section 1030(a)(5)(A). Dkt. No. 1 at ¶ 3. Section 3237(a) of Title 18 provides that any offense "begun in one district and completed in another, or committed in more than one district may be … prosecuted in any district in which such offense was begun, continued, or completed." This is long-standing black-letter law. *See also United States v. Lombardo*, 241 U.S. 73, 77 (1916) ("where a crime consists of distinct parts which have different localities the

[2] Defendants' alternative interpretation of the statute substituting in the phrase "with the intent to" occurs in other subsections of the statute, e.g., § 1030(a)(4) (accessing a protected computer with the intent to defraud), but not in this subsection.

[3] The defendants are also charged with Section 1030(c) sentence enhancements which make the crime charged a felony. This creates two additional elements of 10 or more computers affected or aggregate loss in excess of $5,000, which would have to be proven at trial. *See United States v. Auernheimer*, ___ F.3d ___, 2014 WL 1395670, at *5 (3d Cir. 2014). However, further analysis of these other elements is unnecessary and does not change the outcome.

whole may be tried where any part can be proved to have been done."). This principle is applicable to conspiracy cases as well. *See Hyde v. United States,* 225 U.S. 347, 356-367 (1912) (venue proper against defendant in district where co-conspirator carried out overt acts even though there was no evidence that the defendant had ever entered that district or that the conspiracy was formed there). The indictment in this case alleges multiple overt acts in which damage to protected computers occurred in the Eastern District of Virginia as a direct result of computer transmissions by the co-conspirators targeting these computers with DDoS attacks.[4] *See, e.g.*, on September 19, 2010, a DDoS attack on the website of the Recording Industry Association of America ("RIAA") hosted on computers in the Eastern District of Virginia (Overt Acts ¶ 18); on September 21, 2010, another DDoS attack on the website of RIAA hosted on computers in the Eastern District of Virginia (Overt Acts ¶ 22); on October 29, 2010, another DDoS attack on the website of RIAA hosted on computers in the Eastern District of Virginia (Overt Acts ¶ 58); on December 18, 2010, a DDoS attack on the website of Bank of America which included computers at a data center in the Eastern District of Virginia (Overt Acts ¶ 93); and, on December 24-27, DDoS attacks on the websites of RIAA and Bank of America in the Eastern District of Virginia (Overt Acts ¶¶ 96-97). Dkt. No. 1. Clearly, offense conduct occurred in the Eastern District of Virginia in this case.

[4] Other overt acts describe the co-conspirators discussing and planning other DDoS attacks targeting computers here in the Eastern District of Virginia, *e.g.*, the law firm of DunlapWeaver (Dkt. No. 1, Overt Acts ¶ 41); U.S. Immigration and Customs Enforcement (Dkt. No. 1, Overt Acts ¶ 70); the Central Intelligence Agency (Dkt. No. 1, Overt Acts ¶ 72). The conspirators even discussed harassment of the CEO of RIAA who lived in this District (Dkt. No. 1, Overt Acts ¶ 56).

B. Even if Defendants' Interpretation of the Statute Were Correct, There is Still Venue in This District.

The Defendants invite this Court to misinterpret the statute as they have, and to read the statute as having but one essential conduct element, namely, "'knowingly caus[ing] the transmission of a program, information, code, or command' with the intent to cause damage." Heller MTD at 3. This mis-interpretation of the statute is critical to the defendants' argument. The defendants urge this mis-interpretation to support their claim that damage to computers in this District is only a "circumstance element" and not an essential element of the criminal offense. *See Bowens*, 224 F.3d at 310 ("only the essential conduct elements of an offense, not the circumstance elements, provide a basis for venue"); *see also United States v. Auernheimer*, ___ F.3d ___, 2014 WL 1395670, at *4 (3d Cir. 2014). As noted above, the essential conduct elements of the offense in question clearly establishes venue in this District, but even assuming that the defendants' interpretation of the essential conduct element was correct, their argument that venue is improper here still fails in two ways. First, the natural construction of the statute would include "protected computer" as the object of each clause of the statute including the transmission element. Therefore, even the defendants' interpretation of the statute would more properly read—knowingly caus[ing] the transmission of a program, information, code, or command with the intent to cause damage *to a protected computer*. The essential conduct element would now include the location of the target computer as one of the places where venue would be proper, in this case the Eastern District of Virginia as the locus of several targeted

computers. To read the statute otherwise would suggest that one could violate the statute by simply transmitting a computer command into the void with the hopes that it would somehow find a protected computer to damage. This would be an absurd interpretation of this statute. Statutes are to be interpreted to avoid absurd results. *Chapman v. United States*, 500 U.S. 453, 476 (1991) ("There is nothing in our jurisprudence that compels us to interpret an ambiguous statute to reach such an absurd result. In fact, we have specifically declined to do so in the past, even when the statute was not ambiguous, on the ground that Congress could not have intended such an outcome."). .

Second, venue may be proper where the effects of criminal conduct are felt, if an essential conduct element is itself defined in terms of its effects. *Bowens*, 224 F.3d at 311. Here, even adopting the defendants' reading of the statute, Congress has defined the essential conduct element of transmitting computer commands in terms of its effects on a protected computer, namely, with the intent to cause damage to a protected computer. Therefore, even if damage were not an essential conduct element supporting venue, since the statute defines the transmission element in terms of its effects (damage to a computer), under *Bowens*, venue is still proper wherever one of those targeted protected computers is located.

Conclusion

The defendants would have the Court believe that DDoS attacks targeting and damaging computers in this District results in no venue in this District. That is just not the case. In *United States v. Johnson*, the Fourth Circuit noted that "[i]t is

well accepted that there may be 'more than one appropriate venue, or even a venue in which the defendant has never set foot,' so long as it meets the relevant constitutional and statutory requirement." 510 F.3d 521, 525 (4th Cir.2007) (quoting *Bowens*, 224 F.3d at 309). Those requirements have been met in this case and venue properly lies in the Eastern District of Virginia. Defendants' motions should be denied.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: /s/

Alexander T.H. Nguyen
Jay V. Prabhu
Assistant U.S. Attorneys
U.S. Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Phone: (703) 299-3700
Fax: (703) 299-3980
Email: alexander.nguyen@usdoj.gov
Email: jay.prabhu@usdoj.gov

Richard D. Green
Trial Attorney, U.S. Department of Justice
Computer Crime & Intellectual Property Section

Date: April 24, 2014

CERTIFICATE OF SERVICE

I hereby certify that on April 24, 2014, I electronically filed the foregoing GOVERNMENT'S CONSOLIDATED OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS FOR IMPROPER VENUE with the Clerk of Court using the CM/ECF system, which will send a notification of that electronic filling (NEF), and I have also served by email a copy of the foregoing to the following:

John C. Kiyonaga
john@johnckiyonaga.com

Marina Medvin
marina@medvinlaw.com

James W. Hundley
jhundley@bhnklaw.com

William Loeffler
williamodouglas@aol.com

William Todd Watson
todd_watson@fd.org

John O. Iweanoge, II
joi@iweanogesfirm.com

Elita C. Amato
amato@amatoatlaw.com

Drewry B. Hutcheson, Jr.
hutch365@msn.com

Gregory B. English
gbeuva@gmail.com

Jessica Nicole Carmichael
jcarmichael@pnalaw.com

Gretchen Lynch Taylor
gretchen@taylorlawco.com

Gary H. Smith
smithgh58@aol.com

John Louis Machado
johnmachadoesq@kreative.net

Joseph Abrenio
joseph.abrenio@leclairryan.com

Respectfully submitted,

Dana J. Boente
United States Attorney

By: /s/

Alexander T.H. Nguyen
Jay V. Prabhu
Assistant U.S. Attorneys
U.S. Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Phone: (703) 299-3700
Fax: (703) 299-3980
Email: alexander.nguyen@usdoj.gov
Email: jay.prabhu@usdoj.gov

Richard D. Green
Trial Attorney, U.S. Department of Justice
Computer Crime & Intellectual Property Section

Date: April 24, 2014